Panasonic

SYSTEM LSI Dual Interface RFID

MN63Y1214
Administrator's Manual Ver. 1.0

〈 Non NDA type 〉

Warning and Precaution Regarding to Use of the Technical Information and Semiconductor Described in This Document

(1) In case of providing non-resident with, or exporting the product and technical information described in this document, please comply with the law of the interested state, especially, the law regarding to security export management.

(2) The technical information described in this document describes the representative characteristic of the product and the examples of application circuit, etc, which is not licensed by the intellectual property right or other rights of our company or other companies. Therefore, in case there is any problem arising from the use of said technical information regarding to the property right of a third party, our company should be exempted from any responsibility concerned.

(3) The product described in this document is purposed for its standard usage – common electronic equipment (business equipment, communication equipment, measurement equipment, home electric appliances, etc).
For the customer who considers a special usage – the usage which requires a special quality, liability, might harm human body, that any failure or malfunction might directly threaten human life (for the use of aviation/universe, traffic tools, burning appliances, life support system, safety apparatus, etc) and the customer who considers a usage except for the standard purposed by our company, please have a discussion with the sales contact window of our company in advance. Otherwise, we will not be liable for any defect which may arise later in your equipment.

(4) We appreciate your understanding in case of no advance notice before any change for the improvement, etc of the product and the specification of the product described in this document, due to which, please request to get and confirm the latest written standards and specification sheet of the product in advance when doing final design, purchasing and using it.

(5) When doing design, please use it within the scope of absolute maximum rating, operation guarantee condition (operating power voltage, operating environment, etc). Please make a full discussion to make sure that it will not go beyond the transient state when setting power on/off, switching among all kinds of modes. In case of use under the status beyond guaranteed performance, our company will not be responsible for any failure, or defect of the equipment which might happen later.
In addition, please figure out a systematic countermeasure such as redundancy design, flame propagation countermeasure design, malfunction proof design, etc to prevent the equipment in use from causing physical injury, fire accident, public loss arising from the operation of the product made by our company by considering the failure occurrence rate, failure mode normally estimated regarding to semiconductor product even if in case of the use within guaranteed performance.

(6) In order to prevent failure and variation of characteristic arising from the foreign factors (ESD, EOS, thermal stress, mechanical stress) during the process of customer, or when handling, mounting the product, please keep to the described content of precaution items regarding to use.
In addition, regarding to the product to which moisture-proof packaging is necessary, please keep to the conditions determined when concluding every specification sheet, such as retention period, length of exposure after being unsealed, etc.

(7) We will stiffly refuse the reprint or copy of all or a part of this document without the written authorization of our company.

20100202

Please feel free to contact our sales office or sales department at the end of the document for any inquiries regarding this document and the semiconductor of our company.

PanaXSeries is a registered trademark of Panasonic Semiconductor Solutions Co., Ltd.
The other corporation names, logotype and product names written in this book are trademarks or registered trademarks of their corresponding corporations.

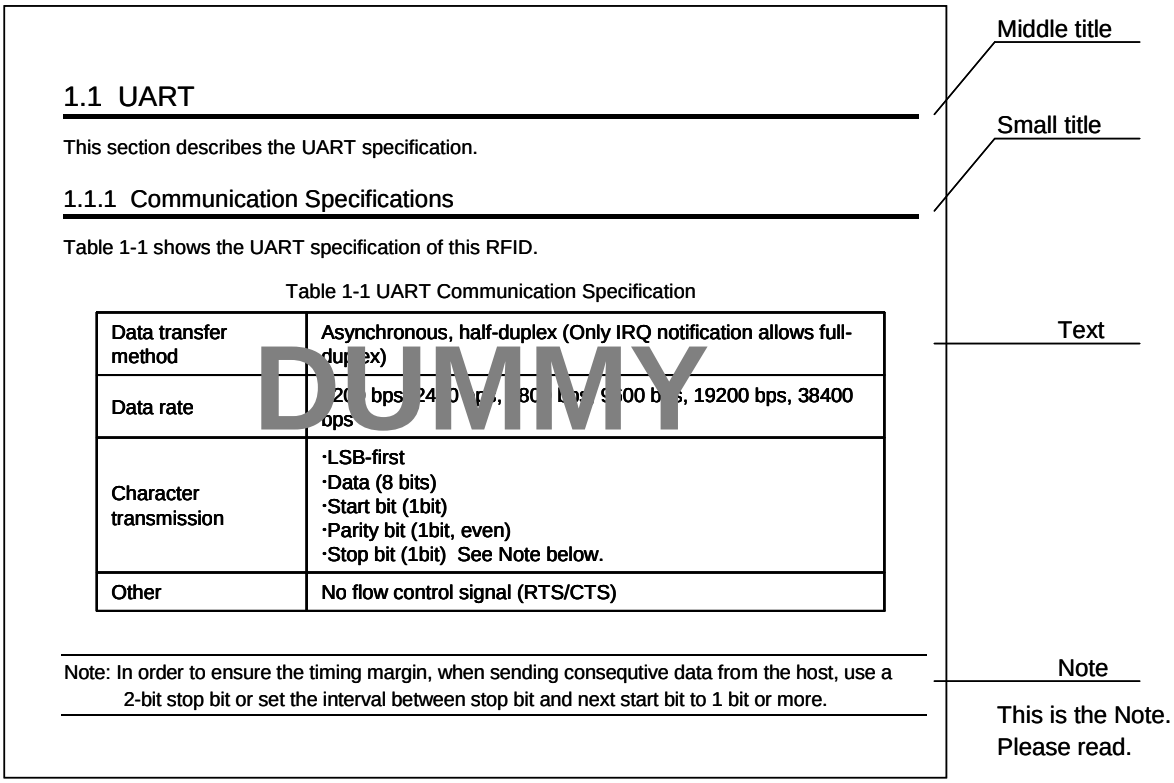
About this manual

■ Organization

These specifications provide important information for users of the MN63Y1213, including an overview and descriptions of functions.

■ Manual Configuration

Each section of this manual consists of a title, main text, and notes. The layout and definition of each section are shown below.


1.1 UART
This section describes the UART specification.
1.1.1 Communication Specifications
Table 1-1 shows the UART specification of this RFID.
Table 1-1 UART Communication Specification
Data transfer method
Asynchronous, half-duplex (Only IRQ notification allows full-duplex)
Data rate
bps, 19200 bps, 38400 bps
Character transmission
·LSB-first
·Data (8 bits)
·Start bit (1bit)
·Parity bit (1bit, even)
·Stop bit (1bit) See Note below.
Other
No flow control signal (RTS/CTS)
DUMMY
Note: In order to ensure the timing margin, when sending consequtive data from the host, use a 2-bit stop bit or set the interval between stop bit and next start bit to 1 bit or more.
Middle title
Small title
Text
Note
This is the Note.
Please read.

■ Finding Desired Information

This manual provides two methods for finding desired information quickly and easily.

1. Consult the table of contents at the front of the manual to locate desired titles.
2. Chapter names are located at the top outer corner of each page, and section titles are located at the bottom outer corner of each page.

Chapter 1 Overview

Chapter 2 System Area

Chapter 3 Password Functionality

Chapter 5 Error Code

Chapter 6 Annex

Contents

Chapter 1 Overview 7

1.1 Overview 8

Chapter 2 System Area 9

2.1 Physical Memory Map 10
2.2 System Area 12
2.2.1 Parameter Specification 12
2.2.2 Parameter setting value selection 16
2.2.3 Parameter Application Timing 17

Chapter 3 Password Functionality 19

3.1 Password Specification 20
3.1.1 Overview 20
3.2 VERIFY Command 21
3.2.1 JISX6319-4 21
3.2.2 ISO/IEC14443 TypeA/TypeB 22
3.3 Access method 24

Chapter 4 Error Code 25

4.1 Error Code 26
4.1.1 JISX6319-4 26
4.1.2 ISO/IEC14443 TypeA/TypeB 26
4.1.3 Serial Interface (I2C) 26

Chapter 5 Annex 27

5.1 Configuring the System Area 28
5.1.1 Precautions 28
5.1.2 Setting Procedures of System Area 29

Chapter 1 Overview

1

1.1 Overview

This is a manual for the administrator of the RFID (Radio Frequency Identification) LSI MN63Y1214, and describes the following:

- System area (Chapter 2)

Describes the information on security in the system area of FeRAM, which is omitted in the User's Manual.

- System command (Chapter 3)

Describes system commands for the administrator.

- Password functionality (Chapter 4)

Provides the password functionality.

- Additional error codes (Chapter 5)

Provides the error codes related to the Administrator's Manual, which are not described in the User's Manual.

- Annex (Chapter 6)

Describes examples of configuring the system area in the manufacturing process.

Chapter 2 System Area

2

2.1 Physical Memory Map

Figure 2-1 shows the physical memory map. The part indicated in bold italic is to be defined in this manual.

Block	Address	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xA	0xB	0xC	0xD	0xE	0xF
0	0x0000	User Area															
1	0x0010	User Area															
2	0x0020	User Area															
3	0x0030	User Area															
4	0x0040	User Area															
5	0x0050	User Area															
6	0x0060	User Area															
7	0x0070	User Area															
8	0x0080	User Area															
9	0x0090	User Area															
10	0x00A0	User Area															
11	0x00B0	User Area															
12	0x00C0	User Area															
13	0x00D0	User Area															
14	0x00E0	User Area															
15	0x00F0	User Area															
16	0x0100	User Area															
17	0x0110	User Area															
18	0x0120	User Area															
19	0x0130	User Area															
20	0x0140	User Area															
21	0x0150	User Area															
22	0x0160	User Area															
23	0x0170	User Area															
24	0x0180	User Area															
25	0x0190	User Area															
26	0x01A0	User Area															
27	0x01B0	User Area															
28	0x01C0	User Area															
29	0x01D0	User Area															
30	0x01E0	User Area															
31	0x01F0	User Area															
32	0x0200	User Area															
33	0x0210	User Area															
34	0x0220	User Area															
35	0x0230	User Area															
36	0x0240	User Area															
37	0x0250	User Area															

38	0x0260	User Area														
39	0x0270	User Area														
40	0x0280	User Area														
41	0x0290	User Area														
42	0x02A0	User Area														
43	0x02B0	User Area														
44	0x02C0	User Area														
45	0x02D0	User Area														
46	0x02E0	User Area														
47	0x02F0	User Area														
48	0x0300	User Area														
49	0x0310	User Area														
50	0x0320	User Area														
51	0x0330	User Area														
52	0x0340	User Area														
53	0x0350	User Area														
54	0x0360	User Area														
55	0x0370	User Area														
56	0x0380	User Area														
57	0x0390	User Area														
58	0x03A0	User Area														
59	0x03B0	User Area														
60	0x03C0	***PASSWORD***														
61	0x03D0	***VCNT***	***VMAX***	-	-	-	IRQBS	IRQBE	HWCF	***CFEN***				***MC***		
62	0x03E0	SC		IDM								PMM		AFI	HW3	HW1
63	0x03F0	RORF			ROSI				SECURITY				TNPRM	HW2	***SL***	***BCC***

Figure 2-1 Physical Memory Map

2.2 System Area

This section describes the system area.

2.2.1 Parameter Specification

This section provides parameters for password in the system area. For information about other parameters, see the User's Manual.

All addresses and block numbers used in this section correspond to the physical address in Figure 2-1.

■ PASSWORD (16 bytes)

It is stored a password for the password certification of the RF communication. The default value is unsettled. In the normal mode (WRITE command) of the RF communication, can be written in the serial communication, but All 0 is read by both RF communication and serial communication.

Table 2-1 PASSWORD Parameter

Address	0x03C0	0x03C1	0x03C2	0x03C3	0x03C4	0x03C5	0x03C6	0x03C7
Default	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX
Address	0x03C8	0x03C9	0x03CA	0x03CB	0x03CC	0x03CD	0x03CE	0x03CF
Default	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX	0xXX

■ VCNT (1byte)

It stores failure count (0x01 - 0x0F) of the password certification by the VERIFY command of the RF communication. It is 0x0F (15 times), but the upper limit of the failure count is understood that it is the same as 0x0F when 0x10 - 0xFF is set. Regardless of the set point of the SL parameter, it is able to rewrite by Host command. Indicated only 1 byte of VCNT at the time of the rewrite, rewrite it. 0x00 is retrieved by the reading of the RF communication. If it is within regular count to be set in VMAX parameter, it is reset by the normal password agreement of the VERIFY command.

Table 2-2 VCNT Parameter

Address	0x03D0
VCNT	D0
Default	0x00

■ VMAX (1byte)

It is set the upper limit of the failure count of the password certification by the VERIFY command of the RF communication. Regardless of an SL state, it is possible to rewrite by Host command. Specified only 1 byte of VMAX at the time of the rewrite, rewrite it. 0x00 is retrieved by the reading of the RF communication.

There is not the upper limit of the failure count; it becomes unlimited when a set point is “0x00”. The response to VERIFY command is replied an error when a set point is 0x01 - 0x0F, if the failure count is reached, and the access to a password protection block becomes the error reply. When a set point is 0x10 - 0xFF, it is an invalid value, becomes 0x0F setting and same handling.

Table 2-3 VMAX Parameter

Address	0x03D1
VMAX	D0
Default	0x00

■ CFEN (4 bytes)

As with BCC, CFEN is a flag data to validate the setting values in the system area of FeRAM. Table2-4 is indicated the valid setting values for system area. Until valid values are written to CFEN and BCC, default values (implemented in hardware) are used for each parameter. For information about the default values, see Section 3.3 in the User's Manual and the descriptions for each parameter in this section.

Table 2-4 Valid CFEN Setting Values for System Area

Address	0x03D8	0x03D9	0x03DA	0x03DB
System area enable setting	0x01	0x23	0x45	0x67

Note: For Password, no default values are provided and the system area values of FeRAM are used regardless of CFEN settings.

Note: In order to enable the written flag data, the RFID's power supplies (both VDDEX and the supply from RF interface) must be turned off once after writes. The data will be enabled after next power-on. In addition, it becomes effective after the self-reset.

Note: Before writing valid setting values to CFEN, write the given setting values to each parameter in the system area of FeRAM. (Default values for each parameter are implemented in hardware.)

■ MC (4 bytes)

MC is a data to control the internal modes of this RFID.

In manufacturing process, when writing the Block 61 data to this area, write the data shown in Table2-5.

Table 2-5 MC Setting Values

Address	0x03DC	0x03DD	0x03DE	0x03DF
System area enable setting	0x89	0xAB	0xCD	0xEF

■ SL (1 byte)

SL is a flag data to lock the system area. Table 2-6 is indicated the SL settings and corresponding values. Setting the SL to MODE1 or MODE2 allows locking the write operation to parameters of the system area.

In case except 0x0F or 0xFF, as for the one of default setting, it is the case that an invalidity level is set in CFEN and SL set point in MODE0. In addition, the system lock state, BCC is unrelated.

Table 2-6 SL Settings and Corresponding Values

Mode	MODE0		MODE1		MODE2	
Setting value (Address: 0x03FE)	0x00		0x0F		0xFF	
Interface to be accessed	RF	Serial	RF	Serial	RF	Serial
PASSWORD(*1)	R/W	R/W	RO	RO	RO	RO
VCNT(*2)	R/W	R/W	RO	R/W	RO	R/W
VMAX(*2)	R/W	R/W	RO	R/W	RO	R/W
IRQBS	R/W	R/W	RO	RO	RO	RO
IRQBE	R/W	R/W	RO	RO	RO	RO
HWCF	R/W	R/W	RO	RO	RO	RO
CFEN	R/W	R/W	RO	RO	RO	RO
MC	R/W	R/W	RO	RO	RO	RO
SC	R/W	R/W	RO	RO	RO	RO
IDM	R/W	R/W	RO	RO	RO	RO
PMM	R/W	R/W	RO	RO	RO	RO
AFI	R/W	R/W	RO	RO	RO	RO
HW3	R/W	R/W	RO	RO	RO	RO
HW1	R/W	R/W	RO	RO	RO	RO
RORF	R/W	R/W	RO	R/W	RO	RO
ROSI	R/W	R/W	RO	R/W	RO	RO
SECURITY	R/W	R/W	RO	R/W	RO	RO
TNPRM	R/W	R/W	RO	R/W	RO	RO
HW2	R/W	R/W	RO	R/W	RO	RO
SL	R/W	R/W	RO	R/W	RO	RO
BCC	R/W	R/W	RO	R/W	RO	RO

R/W: Read/Write, RO: Read Only

*1 Both RF communication and Serial communication, All0 is retrieved at the time of the reading.

*2 The reading by the RF communication, All0 is retrieved.

When a value effective for CFEN is set, it is settable by writing in 0x0F at SL from MODE0 to MODE1 and is settable by writing in 0xFF at SL from MODE0 or MODE1 to MODE2. In addition, the write data to SL is able to write only 0xFF when set it from MODE1 to MODE2.

It is impossible to set it from MODE2 to MODE1. Need to execute an INIT command by serial communication from MODE1 or MODE2 to MODE0. Refer to Chapter 3 for the INIT command.

Note: SL is the flag data for locking the system area.
In order to release the system area that was once locked, dedicated command using the serial
The disclosure of this dedicated command, NDA is required.

In addition, Figure 2-2 illustrates the state transition diagram between system lock modes.

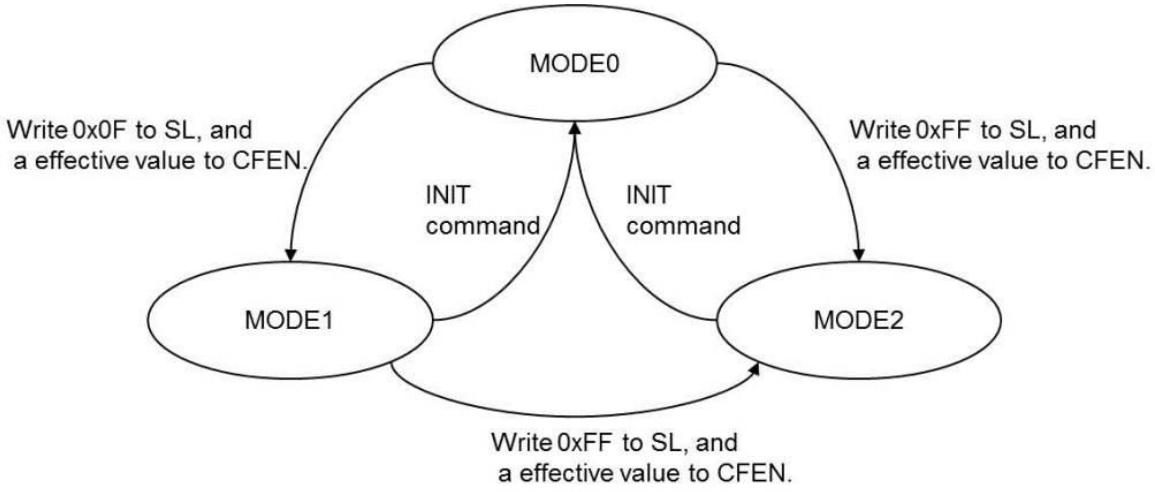


Figure 2-2 State Transition Diagram between System Lock Modes

■ BCC (1 byte)

BCC is a flag data to validate the setting values in the system area of FeRAM. Table 2-7 shows the valid setting value for system area. Until valid values are written to BCC and CFEN, default values (implemented in hardware) are used for each parameter. For information about the default values, see Section 3.3 in the User's Manual and the descriptions for each parameter in this section.

Table 2-7 Valid BCC Setting Value for System Area

Address	0x03FF
System area enable setting	BCC setting value

BCC setting value is obtained by adding the values at 0x03D5, 0x03D6, 0x03D7, 0x03D8 to 0x03EF and 0x03FC to 0x03FD of the system area, byte-by-byte, to the default value 0x00 of 1 byte and subtracting the lower one byte of the calculation result from 0x100.

BCC is calculated by hardware at power-on of this RFID or at a reset.

If the calculation result generates an error, this LSI operates with default values for each parameter and the error state can be read with a response to the RREG command in serial communication.

2.2.2 Parameter setting value selection

Setting of CFEN and BCC is necessary to make each parameter of the system area an existence effect. Show a selective status of each parameter by the combination of CFEN and BCC to Table 2-8.

Table 2-8 Parameter selective status

CFEN		Ineffective value	Effective value	
BCC	(BCC calculation)	voluntary	Ineffective value	Effective value
PASSWORD	No	Default	Default	Setting value
VCNT	No	Default	Default	Setting value
VMAX	No	Default	Default	Setting value
IRQBS	Yes	Default	Default	Setting value
IRQBE	Yes	Default	Default	Setting value
HWCF	Yes	Default	Default	Setting value
CFEN	Yes	(Ineffective value)	(Effective value)	(Effective value)
MC	Yes	-(irrelevance)	-(irrelevance)	-(irrelevance)
SC	Yes	Default	Default	Setting value
IDM	Yes	Default	Default	Setting value
PMM	Yes	Default	Default	Setting value
AFI	Yes	Default	Default	Setting value
HW3	Yes	Default	Default	Setting value
HW1	Yes	Default	Default	Setting value
RORF	No	Default	Default	Setting value
ROSI	No	Default	Default	Setting value
SECURITY	No	Default	Default	Setting value
TNPRM	Yes	Default	Default	Setting value
HW2	Yes	Default	Default	Setting value
SL	No	Default	Setting value	Setting value
BCC	(BCC)	(voluntary)	(Ineffective value)	(Effective value)

2.2.3 Parameter Application Timing

Table 2-9 lists the setting application timings after rewriting parameters in the system area while CFEN is enabled.

Table 2-9 Parameter Application Timing

	A timing at which new parameter setting is applied after rewriting parameters while CFEN is enabled.
PASSWORD	Apply immediately after rewrites.
VCNT	Apply immediately after rewrites.
VMAX	Apply immediately after rewrites.
CFEN	Apply after turning power ON from OFF or self-reset following rewrites.
MC	Apply after turning power ON from OFF or self-reset following rewrites.
SL	Apply after turning power ON from OFF or self-reset following rewrites.
BCC	Apply after turning power ON from OFF or self-reset following rewrites.

Note: Power OFF means power supplies from both VDDEX and RF interface are OFF.

Chapter 3 Password Functionality

3

3.1 Password Specification

This section provides the password specification for this RFID.

3.1.1 Overview

- In system area 0x03C0 to 0x03CF of FeRAM, it sets PASSWORD parameter.
- The PASSWORD parameter is able to write from RF or Host, but the reading is impossible.
  (ALL0 at the time of the reading)
- Performed the password overwrite prevention in SL parameter of the system area.
- Assignment the password protection object in ACC, RORF, SECURITY parameter of the system area of FeRAM.
- Comparison password by VERIFY command (new specifications) and, in the case of correspondence, enable READ/WRITE to the user's area for the following password protection.
- In case of password discordance becomes beyond the regular counts (VMAX parameter setting), the error reply (overflow).
- It is possible to clear the counter value where is mismatched for a password only from a host.

3.2 VERIFY Command

This section describes VERIFY command in detail.

3.2.1 JISX6319-4

■ Overview

VERIFY is command for password certification.

■ Command messages

● Format

Code	PICC identifier	The number of Service files identifier(k)	List of Service Files identifier	The number of block(m)	Block lists	Block data
1 byte	8 bytes	1 byte	2×k bytes	1 byte	2×m or 3×m bytes	16×m bytes

● Data Field

Field	Setting	Remarks
Code	0x08	
PICC identifier	Refer to the PICC identifier which is acquired that is user's manual "4.2.6.1 REQ command".	
The number of Service files identifier(k)	The number of Service files Setting range: 0x01(1) to 0x0B(11)	An error replies other than a following setting range
List of Service Files identifier	Don't care (Example: 0x0900)	If not to specify all the value of the same service file at the time of plural service designation, an error replies.
The number of block(m)	0x01	An error replies other than a following setting range
Block lists	0x000001	
Block data	16bytes	

■ Response messages

● Format

Code	PICC identifier	Status Flag 1	Status Flag 2
1byte	8bytes	1byte	1byte

- Data Field

Field	Output	Remarks
Code	0x09	
PICC identifier	See User's Manual 4.2.5.2 PICC (Proximity IC card) Identifier	
Status Flag 1	See User's Manual 4.2.5.8 Status Flag	
Status Flag 2	See User's Manual 4.2.5.8 Status Flag	

VERIFY command is the command that limited the number of the blocks of the WRITE command, block lists, and the setting value of block data like above table.

3.2.2 ISO/IEC14443 TypeA/TypeB

■ Overview

VERIFY is command for password certification.

■ Command messages

- Format

CLA	INS	P1	P2	Lc	Data
1 byte	1 byte	1 byte	1 byte	1 byte	16 bytes

- Data Field

Field	Setting	Remarks
CLA	0x00	An error replies other than 0x00
INS	0x20	
P1	0x00	An error replies other than 0x00
P2	0x00	An error replies other than 0x00
Lc	0x10 Byte length of the Data part	An error replies other than 0x10
Data	Password	

■ Response messages

- Format

SW1	SW2
1 byte	1 byte

- Data Field

Field	Output	Remarks
SW1	See User's Manual 4.3.8.7 Status Word	
SW2	See User's Manual 4.3.8.7 Status Word	

3.3 Access method

Figure 3-1 shows the access method to the password domain set in SECURITY parameter of the system area.

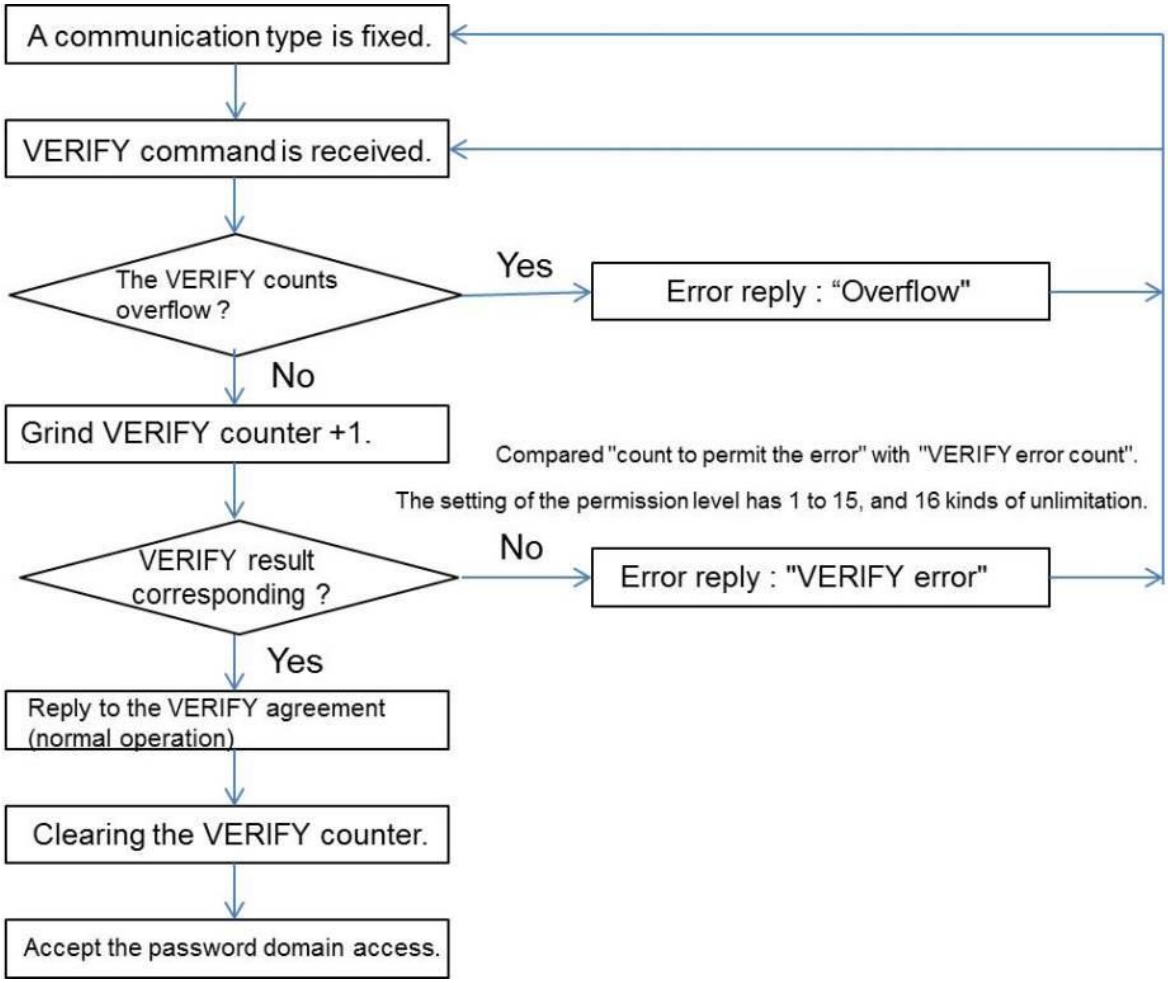

A communication type is fixed.
VERIFY command is received.
The VERIFY counts overflow ?
Yes
Error reply : “Overflow"
No
Grind VERIFY counter +1.
Compared "count to permit the error" with "VERIFY error count".
The setting of the permission level has 1 to 15, and 16 kinds of unlimitation.
VERIFY result corresponding ?
No
Error reply : "VERIFY error"
Yes
Reply to the VERIFY agreement (normal operation)
Clearing the VERIFY counter.
Accept the password domain access.

Figure 3-1 Access method to the password domain specified in SECURITY

Chapter 4 Error Code

4

4.1 Error Code

This section provides the error codes related to this Administrator's Manual by interface, which are not described in the User's Manual.

4.1.1 JISX6319-4

Table 4-1 lists the meanings of statuses for JISX6319-4, which are not described in the User's Manual.

Table 4-1 Status Flag

Status flag 1	Status flag 2	Meaning	Description
0xFF	0xA5	Block count specified error	When writing to password area, the data size was other than 16 bytes.
0xFF	0x60	Self-checking error	・ Access to the password protection domain in password non-certification. (VERIFY unsuccessfulness) ・ The password of the VERIFY command is wrong. ・ The failure count of the VERIFY command exceeds the regular value.

4.1.2 ISO/IEC14443 TypeA/TypeB

Table 4-2 lists the meanings of statuses for ISO/IEC14443 TypeA/TypeB, which are not described in the User's Manual.

Table 4-2 Status Word

SW1	SW2	Meaning	Description
0x69	0x82	Access authority error	Access to the password protection domain in password non-certification (VERIFY unsuccessfulness).
0x690x6F	0x83	Password control error	・ The failure count of the VERIFY command exceeds the regular value.
0x69	0x84	Password certification error	・ The password of the VERIFY command is wrong.

4.1.3 Serial Interface (I2C)

Table 4-3 lists the meanings of statuses for serial interface (I2C), which are not described in the User's Manual.

Table 4-3 Status

Value	Meaning	Description
0x26	Command parameter error	・ Write access to the system area (SL function) was performed while the system is locked.

Chapter 5 Annex

5

5.1 Configuring the System Area

When configuring the system area in the manufacturing process, you must follow some precautions. This section describes the precautions and the setting procedures.

5.1.1 Precautions

Precautions are as follows:

- 1: When configuring the system area by using a contactless reader/writer while the contactless reader/writer turns carrier off every time a command is issued, it is necessary to observe the writing unit and order. For example, the parameters (e.g., SC, IDM) related to communication command can change their values when configuring the system area or when writing a valid value to CFEN (*). In this case, when writing a valid value to CFEN, writing data to Blocks 61 to 63 by a single command prevents the system area setting from being complicated.
- 2: Data must be written to PASSWORD (Block60) in units of one block. Use a WRITE command to write a block (16 bytes) of plaintext.
- 3: All-0 is always read from PASSWORD (Block60), regardless of the value of written data. When verifying data writes to these blocks, check if the RFID responds normally to the VERIFY command.

(*) As an example, we assume that data is written to Block61, Block62 in units of one block while the contactless reader/writer turns carrier off every time a command is issued.

- Description

(1) Writing toBlock61: Write a valid value to CFEN (CFEN has invalid value before executing (1)).

(2) Writing toBlock62: Write a given value to IDM.

When data is written in the order of (1) and (2), the value of IDM changes as follows.

Before executing (1): default value (0x02FE000000000000);

After executing (1): the value of FeRAM that is not written is set since (2) has not yet been executed.

When using READ and WRITE commands based on JISX6319-4, IDM must be specified. Although you can acquire the IDM of this RFID using a REQ command, it is necessary to insert a REQ command between (1) and (2) to acquire IDM and set that IDM to the IDM to which a value is to be written by a WRITE command in (2).

When writing a valid value to CFEN, it is recommended to use a single WRITE command for Blocks 61 to 63.

5.1.2 Setting Procedures of System Area

This section provides two setting procedures of the system area (Steps 1 and 2).
Figure 5-1 shows Step 1 (writing all data only in one process).

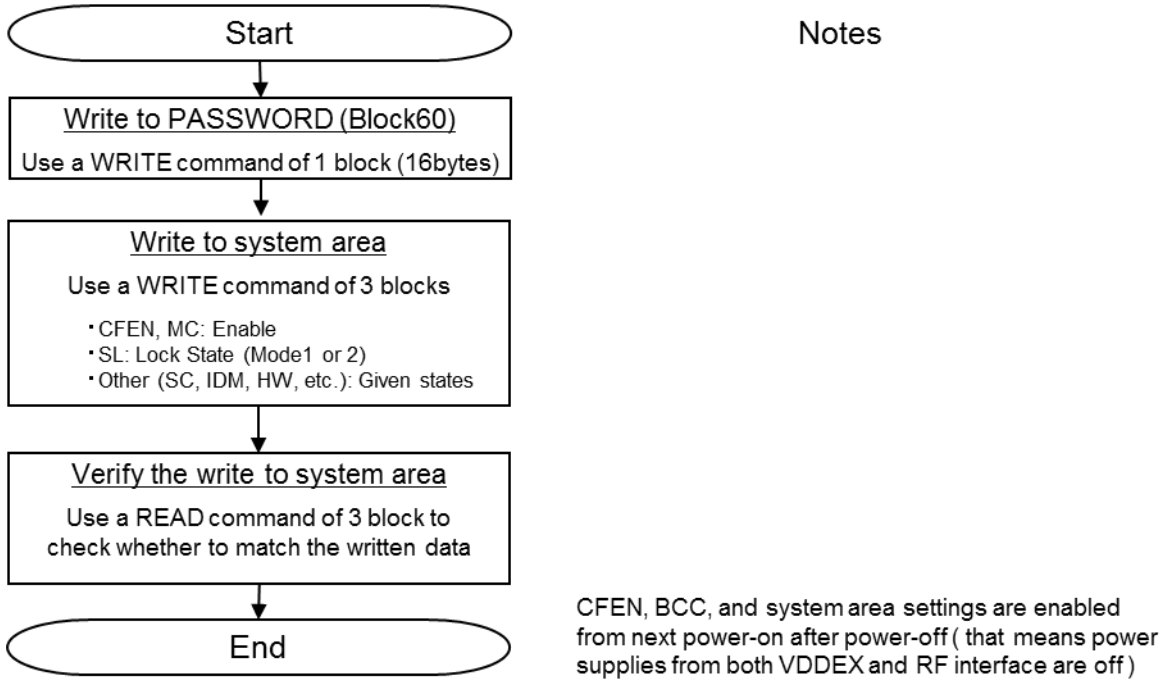

Start
Write to PASSWORD (Block60)
Use a WRITE command of 1 block (16bytes)
Write to system area
Use a WRITE command of 3 blocks
・CFEN, MC: Enable
・SL: Lock State (Mode1 or 2)
・Other (SC, IDM, HW, etc.): Given states
Verify the write to system area
Use a READ command of 3 block to check whether to match the written data
End
Notes
CFEN, BCC, and system area settings are enabled from next power-on after power-off (that means power supplies from both VDDEX and RF interface are off)

Figure 5-1 System Area Setting Procedure (Step 1)

Figure 5-2 shows Step 2 (writing all data in two processes). This step, for example, can be applied to the case in which first you configure the system area and then configure the user area in another process.

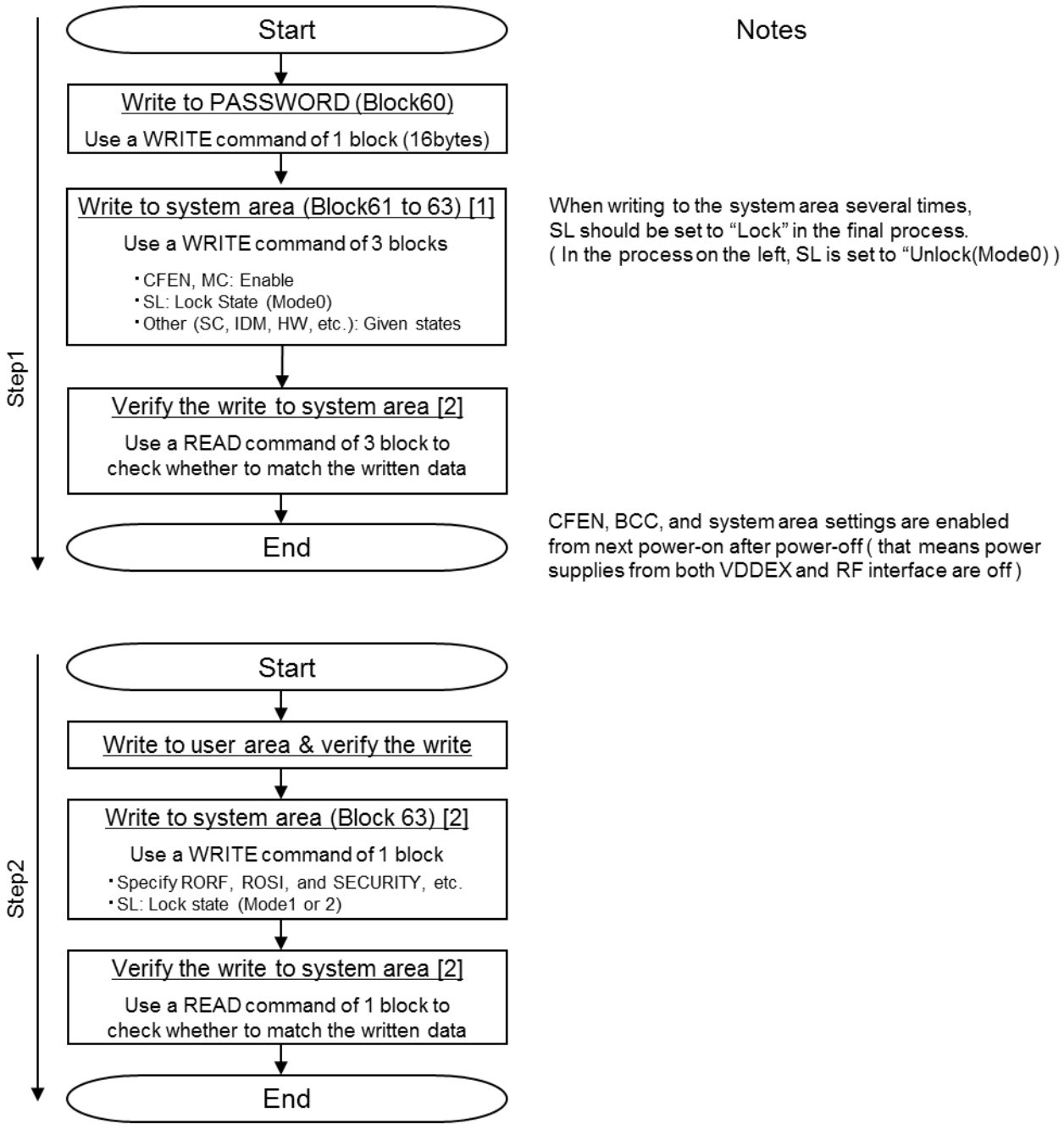

Step1
Start
Write to PASSWORD (Block60)
Use a WRITE command of 1 block (16bytes)
Write to system area (Block61 to 63) [1]
Use a WRITE command of 3 blocks
・CFEN, MC: Enable
・SL: Lock State (Mode0)
・Other (SC, IDM, HW, etc.): Given states
Verify the write to system area [2]
Use a READ command of 3 block to check whether to match the written data
End
Notes
When writing to the system area several times, SL should be set to “Lock” in the final process. (In the process on the left, SL is set to “Unlock(Mode0))
CFEN, BCC, and system area settings are enabled from next power-on after power-off (that means power supplies from both VDDEX and RF interface are off)
Step2
Start
Write to user area & verify the write
Write to system area (Block 63) [2]
Use a WRITE command of 1 block
・Specify RORF, ROSI, and SECURITY, etc.
・SL: Lock state (Mode1 or 2)
Verify the write to system area [2]
Use a READ command of 1 block to check whether to match the written data
End

Figure 5-2 System Area Setting Procedure (Step 2)

Revision History

Revisions of MN63Y1214 administrator's manual (non NDA) is the following.

Revised on Sep 24, 2014

Purpose	Version 1.0			-		
	Page	Section	Comments	Page	Section	Comments
-	-	-	Provisional version	-	-	-

MN63Y1214
Administrator's Manual

Sep 24, 2014, Version 1.0

Issued by
Panasonic Semiconductor Solutions Co., Ltd.

Edited and produced by
Panasonic Semiconductor Solutions Co., Ltd.

© Panasonic Semiconductor Solutions Co., Ltd. 2014